

SUBMISSION TO ONLINE SAFETY BILL COMMITTEE

May 2022

1. We welcome the opportunity to make a submission to the Online Safety Bill Committee and set out, in summary below, our response to the Bill and our proposals for amendments.
2. At Carnegie UK, our focus is on improving collective wellbeing and reducing the harm experienced by individuals and to society. We first devised the "statutory duty of care, enforced by a regulator" approach in original work in 2018 and drafted a complete Bill¹ to implement the regime in 2019. Our extensive work to date on Online Harms and the Online Safety Bill can be found on our website². We were pleased to note that many of the recommendations we made to the Joint Committee in our oral evidence,³ our written submission⁴ and our extensive suggestions for amendments⁵ to the draft Bill have been addressed by the Government.
3. Our approach is to target the systems and processes a company operates that create a risk of harm. A harmful piece of content on its own will have very low impact unless the company running the platform allows it to reach people who might be harmed. Companies can do this deliberately through badly run algorithms, or incentives to post harmful things; or they can allow users to manipulate their services to harmful ends. Some aspects of a service can be harmful independent of content – for example, constantly alerting children who might have gone to sleep, complaints systems that don't work, sign-up systems that allow repeat offenders or bots, etc, to create new accounts. Tackling these systems and processes has a systemic effect – and is more protective of fundamental rights, such as freedom of speech – rather than just playing infinite whack-a-mole with bad bits of content.
4. As set out in our initial analysis of the final Bill⁶, however, we still have many concerns and proposed amendments that we will continue to work on – with fellow civil society organisations and/or with Parliamentarians from all parties – during the passage of the Bill through the House. We would be happy to provide further information to the Committee members during the course of their deliberations.

Headline issues

5. Overall, we welcome the improvements from the draft Bill that make the regime work better, giving OFCOM more powers to investigate and tackle harmful systems in companies (through better risk assessment). We note the fact that victims now get more protection – such as mea-

1 Carnegie UK Trust – a draft online harm reduction bill Woods, Perrin, Walsh December 2019 https://d1ssuo70pg2v9i.cloudfront.net/pex/pex_carnegie2021/2019/12/05125320/Carnegie-UK-Trust-draft-ONLINE-HARMS-BILL.pdf

2 <https://www.carnegieuktrust.org.uk/programmes/tackling-online-harm/>; all our most recent and relevant work on the OSB is brought together in one place here: <https://www.carnegieuktrust.org.uk/carnegie-uk-online-safety-bill-resource-page/>

3 <https://committees.parliament.uk/oralevidence/2794/pdf/>

4 <https://committees.parliament.uk/writtenevidence/39242/pdf/>

5 <https://www.carnegieuktrust.org.uk/blog-posts/the-online-safety-bill-reducing-complexity-establishing-a-foundation-duty/>

6 https://d1ssuo70pg2v9i.cloudfront.net/pex/pex_carnegie2021/2022/03/20161959/Online-Safety-Bill-Carnegie-UK-initial-analysis.pdf

asures on protecting children from pornography and (some) users from online fraud and scams.

6. But the Bill remains too complex – this will lead to ineffective regulation for both service users and companies. The regime, as designed, also relies upon vital yet unknown details in secondary legislation and OFCOM codes of practice/guidance. While technical details may appropriately be deferred to codes and guidance, central policy issues should not be. The Bill's structure and drafting still pushes services to addressing harmful content (often in a palliative rather than proactive way), rather than harmful systems, business models and algorithms (which is a more lasting and systemic approach). We recommend that consolidating the focus on systems would make the regime more effective and better protect fundamental rights.
7. There is also a major concern that the route to the start-up of the regime is Byzantine and lengthy. The regime is unlikely to be fully operational until at least 2024. This leads to delayed protection for users and uncertainty for companies. The Government should bring some aspects forwards by writing well-understood aspects of harm into the Bill.
8. The regulator plays a crucial role in the regime; to respect international standards for the protection of freedom of expression, its independence needs to be safeguarded.

Specific recommendations for amendments

9. We explore these issues in more detail below and we will share our amendments with the Committee as soon as they are ready.
 - **Categorisation:** despite criticism from the Joint Committee and others, the Government is sticking with rigid categories of companies to which the rules apply largely based on size. This is a major hole in a regime that aims to be based on risk. It is wrong to suppose that smaller size means lower risk: users of these platforms still require protection. We recommend that categories should be more flexible, paying particular attention to risk.
 - **Secretary of State powers:** there is still too much unjustified intrusion by the executive and Parliament into the work of the independent regulator, which goes against international norms for communications regulation. We suggest that the Secretary of State's powers to direct OFCOM on the detail of its work (such as codes) are removed. For national security, Government should have carefully constrained powers. OFCOM's Board needs to be bolstered with suitable (vetted) expertise to oversee National Security issues.
 - **Harms to adults:** priority content that is harmful to adults will not be known until the Secretary of State brings forward secondary legislation. It will be difficult for Parliament to assess the impact of the Bill without an indication from the Government as to what it intends. We suggest that the Government should list harms both to children and adults in a new Schedule 7(a) and 7(b), and explicit recognition of the position of minoritised groups – and their freedom of expression – should be included in the regime.⁷
 - **Risks to vulnerable people** – women, members of ethnic or religious minorities, disabled people need better protection; some small changes to risk assessments can easily bring risks to people who have a high innate vulnerability into OFCOM's scope.
 - **Trafficking offences:** human trafficking is a serious omission from Schedule 7 and should be rectified; and advertising, which is significant for indentured servitude, should clearly be in scope for that offence. Amendments here should also include organ trafficking and animal trafficking.
 - **Coordination with other regulators:** the Government is on the cusp of creating a powerful network of regulators, but the Bill does not create powers for domestic inter-regulator coop-

⁷ Along with other civil society partners, charities and academics we have recently launched a Code of Practice to address online Violence Against Women and Girls (VAWG) with a view to this demonstrating how such a cross-cutting, practical approach could ensure greater mitigation of the risk of harms experienced by this group. The Code of Practice is here: <https://www.endviolenceagainstawomen.org.uk/wp-content/uploads/2022/05/VAWG-Code-of-Practice-16.05.22-Final.pdf>

eration. The system must work effectively between these regulators if it is to protect users. The Government should give clear powers to OFCOM to ensure that case files can flow between regulatory systems in accordance with the law.

- **Fraud:** the scope and effect of the new fraudulent advertising powers is too limited. Fraudulent advertising has the same impact on victims wherever they encounter it: the new powers should make all companies run an effective system to mitigate fraud.

Detailed analysis

Issue: systems vs content

10. The Bill is an improvement on the draft Bill, making subtle but important changes to reinforce risk-based regulation of systems rather than simply palliative 'take down'. The system that delivers the content (to millions of people, to those who didn't ask for it, to those who might be vulnerable to it) is more impactful than the content itself. The Government will apply the regime mainly based on size categories – smaller companies will have lower risk management obligations even if they have a high risk of harm.
11. Our work to describe and advocate for a duty of care regime for online harm reduction⁸ has always been rooted in our belief that systemic, risk-based regulation - such as that which is established in countless other sectors - is the most appropriate approach for the online environment. This requires companies to account for, and mitigate, the harm that arises from the design and operation of their systems rather than focusing on individual items of content.
12. Compared to the draft Bill, the approach is now more clearly systems-based. But the structure of the Bill, the addition of content-specific new sections, and its drafting still pushes services to addressing harmful content, rather than systems - including the business model and algorithms. The focus in the safety duties is on 'regulated' content, a definition which is limited to content that is generated by users (clause 49): this then raises the question as to whether the harms that are triggered by the design, operation or features of the service (i.e. the systemic features of the service rather than the individual items of content themselves that that are hosted on the service) will fall in scope.
13. There is a welcome emphasis that the safety duties on illegal content and children "apply across all areas of a service, including the way it is operated and used as well as content present on the service" (Cl 9(4) and 11(4) respectively). This language is not, however, replicated in relation to content that is harmful to adults. The expanded definition of "harm" in the Bill (clause 187) refers to the "the manner of [content's] dissemination (for example, content repeatedly sent to an individual by one person or by different people)". But whether this is sufficient to ensure protection for adults given the omission, remains to be seen.
14. Another issue in this context is that the fact of dissemination - in the context of the children's safety duty - is specifically excluded in relation to some of the duties: 11(3) (prevention from encountering content) and 11(5) (terms of service in relation to clause 11(3)). There is some degree of tension between this and clause 11(4). This ties in with our earlier concern about the focus on content rather than also taking account of the role of the services.
15. **Further amendments to consolidate its focus on systems would make the regime more effective** and provide reassurance to those worried about its impact on free speech.

Risk assessments

16. The requirement that risk assessments must now be "suitable and sufficient" is an improvement. But the language chosen throughout the Bill pushes platforms mainly to addressing the immediate problem - that is the content - rather than the underlying causes and exacerbating factors of platform design. (For example, the specific duties in clause 9(3) (takedown of content and minimisation) can be seen this way.) As a result, the guidance and codes of practice that will come from OFCOM take on a higher significance.
17. The definition of harm itself is modified to be equivalent to "risk of harm and potential harm" which is important given the centrality of risk assessments (which take place before any harm has occurred) to the regime (clause 187). OFCOM can carry out a broadly based risk assessment of all harms. This assessment – largely unchanged from the draft Bill - underpins the entire regime. Here, there remains a welcome focus upon the "characteristics" of the service (that is functionalities, user base, business model, governance and other systems and processes) rather than just the content. A significant and positive change to risk assessment in the regime is the inclusion of specific provisions allowing OFCOM to take action against deficient risk assessments.
18. Nonetheless, there are some problems with the OFCOM clause 83 risk assessment. A risk assessment regime has to take account of people's susceptibility to harm. The Bill laudably focusses on children, a group that is obviously more susceptible. But other large groups in the population (including women, people in ethnic or religious minorities, disabled people) are also more vulnerable to harm. They are not properly recognised in the Bill and are excluded from OFCOM's initial clause 83 risk assessment that sets up the regime. It would greatly help companies if OFCOM were tasked to assess risks to such groups and provide a foundation for companies to act upon – a simple amendment should resolve this.
19. OFCOM's initial risk assessment (and other risk assessments) also miss an opportunity to explicitly include people who might be vulnerable as a result of belonging to more than one vulnerable group and to address the impact of intersectional abuse. OFCOM's risk assessment is required to consider people who may be members of a singular group, but not of two or more groups.
20. Finally, with the removal of the exemption for paid-for advertising in the Bill, ad delivery systems in general may be in scope and relevant to the risk assessment and risk mitigation duties. This we feel to be potentially an important positive step given the role of the advertising funding and the overall business model in supporting certain types of problematic harms. Note, however, that the definition of "search content" excludes "paid-for advertisements" (cl 51(2)(a)), which is a little odd given that this is the type of content over which search engine providers would have the most control. It brings a gap into the protection of children, as products and services that are harmful to children can still be advertised to them via the search engines; the children's risk assessment duty (cl 25) and linked safety duty (cl 26) will not affect paid-for advertising because it falls outside the content affected by the duty.

Categorisation of services

21. By retaining the categorisation of services - which we have argued against previously, as did the Joint Committee - the risk-based regime does not apply across the board and will lead to gaps in enforcement and the likelihood of harms arising and proliferating unchecked on smaller, but potentially fast-growing platforms, before the process for re-categorising them can kick in. Furthermore, companies will not know which category of service they fall into until after the Secretary of State has published definitions on thresholds and laid these as secondary legislation; and as a result they will not know all the duties that could apply to them. This will also lead to delays in the regime being fully enforced.
22. We recommend that the 'category' system is adjusted to become a proportionate, risk-based one. Very large size itself can be an absolute indicator of risk and using very large size as a

proxy brings administrative simplicity, but it is wrong to suppose that smaller size means lower risk.

Future-proofing

23. A duty of care focused on risk-assessment and outcomes would enable both flexibility in a new regulatory regime, as well as futureproofing. The complexity and specificity that has been worked into the new draft of the Bill – partly to account for demands for greater clarity on scope, for example – has an impact on its ability to take account of future, as-yet-unknown harms. With regard to the metaverse, this is a cause for concern.
24. We would encourage the Government to provide more clarity on its assertions that the Bill will cover the metaverse. As we have previously written⁹, it seems likely that a user-to-user regime would encompass the metaverse. There are two sets of questions arising: do the lists of measures in the safety duties seem appropriate for the dynamic, real-time environment of the metaverse? If harms that require action are described by reference to current criminal offences, is there a danger that those offences will themselves become outdated (consider a sexual assault on an avatar)? Of course, the Bill provides for updating but, in the case of the need for new criminal offences, how long will this take? This is not a problem with a systems-focussed regime itself but more generally illustrates the difficulties of relying on lists of types of content in terms of keeping the regime relevant. We believe that gaming is included but it would be helpful for the Government to confirm this; some online computer games closely resemble a metaverse and rely on user-generated content.¹⁰
25. There is a process for reviewing new categories of content that are harmful to children and harmful to adults; but, in the end, it requires secondary legislation. The Secretary of State process for adding in new harm areas is cumbersome (see below). In TV, radio advertising and cinema regulation, the regulator – based on research – can move to combat novel harms because it was given the job of dealing with harmful content as a general category (without further specification), and it has held parliament's confidence for decades.

Issue: reliance on secondary legislation

26. We have concerns, shared with many other organisations, that the scope of protection offered by the Bill will not be clear until after secondary legislation¹¹. 'Priority harms' are central to understanding the Bill's impact; but, while there is a preliminary list of Priority Offences in schedules 5- 7, the same clarity is not available for the other two pillars of the Bill: priority content harmful to adults, and both primary priority content and priority content for children. These areas are critical for victims seeking to understand if the Bill will protect them in future, as well as for companies that might have to manage these risks. We recommend that the Government should add the categories of priority content for both content harmful to children and to adults as a new Schedule 7(a) and 7(b).
27. There is also a lack of clarity about what companies will be expected to do to comply with the regime: this will follow in OFCOM guidance and codes of practice which cannot be produced or consulted upon until after Royal Assent. This is compounded by the lack of clarity around categorisation (see above), where we believe the Government should publish a provisional list of the large and small platforms which the Government and OFCOM considers pose the highest risk of harm and to which the most rigorous risk assessment will apply. This gives some certainty to companies and service users.

⁹ <https://www.carnegieuktrust.org.uk/blog-posts/regulating-the-future-the-online-safety-bill-and-the-metaverse/>

¹⁰ Many 'first person' games change dynamically as the user moves a character in response to other users' movement of their characters. It can be argued that this is user-generated content.

¹¹ Carnegie supported Lord McNally in his 2020 PMB to require OFCOM to produce a report before legislation to give clarity on areas of risk of harm, guidelines etc. and inform debate. Sadly the government ignored this. Online Harms Reduction Regulator (Report) Bill [HL] (HL Bill 22) https://publications.parliament.uk/pa/bills/lbill/58-01/022/5801022_en_2.html#l1g1

28. The process used to make regulations largely requires the affirmative process. This is an improvement on the draft Bill but still does not allow Parliament the same freedom to consider the substance of the text as when matters are dealt with by primary legislation and suffers from a long lag after Royal Assent.
29. As a result of the amount of the regime that is dependent on secondary legislation and/or further decisions from the Secretary of State, the regime will not start working properly until at least 2024: the Government must reduce the wait for the downstream work and bring some aspects forwards – perhaps, for example, making companies' terms and conditions on terrorism, illegal content and protecting children, enforceable from Royal Assent.

Issue: The Secretary of State's powers are still too broad

30. Compared to the broadcasting regime, there is considerably more intrusion by the executive and Parliament into the work of the independent regulator. We have written extensively¹² on why this was problematic in the draft Bill – and it remains so here. It's an international norm in democracies for the executive not to interfere in day-to-day communications regulation. The UK has signed up to many international statements in this vein, as recently as April 2022 at the Council of Europe:¹³

*'media and communication governance should be independent and impartial to avoid undue influence on policy making, discriminatory treatment and preferential treatment of powerful groups, including those with significant political or economic power.'*¹⁴

31. Clause 40 permits the Secretary of State to direct OFCOM to change a code of practice. Whilst the draft Bill permitted this 'to ensure that the code of practice reflects Government policy', clause 40 specifies that any code may be required to be modified 'for reasons of public policy'. While this is more normal language, it is not clear in practice what the difference between the two sets of wording is. Implicitly it seems that this excludes 'national security or public safety', which are specifically dealt with in relation to the CSEA and terrorism codes in clause 40(1)(b). This provision would be unnecessary, given clause 40(1)(a) applies to any draft code include CSEA/terrorism, if public policy were to cover national security or public safety. Different rules apply in relation to CSEA and terrorism codes in that they are reviewed¹⁵. There appears to be no Parliamentary control over this process nor oversight by a competent body such as the National Police Chiefs Council or Directors of Public Health. Moreover, clause 40 sets up a form of endless ping pong where the Secretary of State can simply keep rejecting OFCOM's advice on making SIs, ad-infinitum. OFCOM is obliged to give evidence-based advice and has a very strong track record in doing so, with substantial research capability. We see no justification as to why this power is necessary.
32. The Secretary of State should be able to give high-level guidance on national security issues to the regulator, but not interfere in its detailed work such as codes, guidance and enforcement strategy (see e.g. cl 146, 147). Flagging of a problem is different from saying how it should be resolved, which should be a matter for OFCOM: this is an important free speech principle. **We strongly recommend that the Secretary of State's powers to instruct OFCOM should be trimmed back to national security alone and will publish an amendment on this shortly.**
33. The public policy and public safety sections of Clause 40 should be deleted. OFCOM should have sufficient capability to assess and discuss national security issues with the Government. When public safety issues become sufficiently serious to allow the Government to issue directions to a regulator (such as COVID) we suggest that they are national security issues.
34. In addition, the Secretary of State has powers to amend the Online Safety Objectives (Schedule 4, paragraph 7) – and indeed the Bill (clause 173) – by regulations too. The new relationship between intelligence services and OFCOM (see clause 99) is now codified but with no oversight. And also –

12 <https://www.carnegieuktrust.org.uk/blog-posts/secretary-of-states-powers-and-the-draft-online-safety-bill/>

13 Recommendation CM/Rec(2022)11 of the Committee of Ministers to member States on principles for media and communication governance (Adopted by the Committee of Ministers on 6 April 2022) https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a61712

14 Recommendation CM/Rec(2022)11 of the Committee of Ministers to member States on principles for media and communication governance (Adopted by the Committee of Ministers on 6 April 2022) https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a61712

while protecting security advice is necessary - the caveat that allows this as a reason for redacting information from reviews of codes (clause 43 (6)) does not have any oversight. Who will ensure that it is only the national security/public safety relevant content that has been legitimately removed or obscured before publication?

35. We recommend that OFCOM's board should be strengthened to have oversight of the Secretary of State's power to intervene on national security – with suitably cleared members in a subcommittee.

Issue: scope of harms covered by the Bill

36. In the draft Bill the scope of harms was limited to those directly affecting individual people, not wider harms to society such as sale of arms, racism, trading in drugs etc. The changes to the Bill to include a number of criminal offences now listed in Schedule 7 (such as fraud; sale of a realistic imitation of firearms) mean that some priority illegal harms include areas of harm which are not specifically directed at individuals. The new definition of harm in the Bill may also raise the possibility for societal harm to be included, as it recognises that members of a group can be affected by comments directed at another member of a group. In addition, societal harms that could be harmful to adults could equally, if not more so, be harmful to children. However, (as mentioned above), this will not become clear until the secondary legislation is brought forward with regards to content harmful to adults and children.
37. We also have some concern that the overarching risk assessment for adults in clause 12 (covering only category 1 companies), which expects services to consider the fact that some groups are more likely to encounter harmful content and behaviour and are more likely to be harmed by it (cl 12(5)(d)), is constrained by the scope of "harmful content" (as defined in 53 and 54), and by the constraints on Ofcom's risk assessments and risk profiles (cl 83). As noted above, there is a quantitative threshold for determining which content is harmful (and therefore to be taken into account in the risk assessment) which might not well serve smaller groups. There is no recognition here that some groups might be peculiarly exposed to risk of harm. OFCOM is not expressly mandated when assessing risk to recognise the different level of risk to different groups (or those with intersecting identities); moreover, it must ignore non-designated content harmful to adults.
38. Protecting adults from abuse is important in ensuring that there is free speech for all. The UN Special Rapporteur for Freedom of Expression has noted the chilling effect of misogynistic abuse¹⁵ and the European Court of Human Rights has recognised the positive obligations on signatory states to take action, "enabling them to express their opinions and ideas without fear".¹⁶ As regards the rights of speakers, it is important to note that the regime does not require take down here, and David Kaye when special rapporteur for freedom of expression, emphasised that focussing on a range of interventions was a more proportionate, rights respecting approach.
39. These gaps need to be addressed as the Bill passes through Parliament:
- Mis/disinformation: given the level of evidence-based concerns about the scale and impact of this - which are comparable to those expressed by campaigners in relation to e.g. fraud and scams, or anonymity - it is difficult to understand why the Government rejected the Joint Committee's recommendations in this area. There are two significant disinformation issues that the Bill does not address: disinformation supported by state actors; and COVID disinformation. Several unaccountable civil service teams (such as the Counter-Disinformation Unit¹⁷, the Government Information Cell¹⁸, and the Rapid Response Unit¹⁹) exist to nudge service providers on these issues but we have no record of their effectiveness. The groups do not publish their logs of action to any external authority for oversight of the things they are raising with companies using the substantial privileged authority of HMG nor do they publish the effectiveness of these actions. Nor as far as we know are

15 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, (A/74/486), 19 October 2019, para 51, available: <https://www.undocs.org/A/74/486>

16 Dink v. Turkey, nos. 2668/07, 14 September 2010, para 137).

17 <https://committees.parliament.uk/publications/1280/documents/11300/default/>

18 <https://www.cityam.com/foreign-office-launches-crack-unit-to-counter-kremlin-misinformation-on-social-media/>

19 <https://webarchive.nationalarchives.gov.uk/ukgwa/20200203104056/https://gcs.civilservice.gov.uk/news/alex-aiken-introduces-the-rapid-response-unit/>

they rooted in expert independent external advisers. This very direct state interference in the media gives rise to concerns. The Government should reform this system and bring disinformation firmly into the scope of the regime and put the functions carried out by the disinformation cells under OFCOM's independent supervision.

- Human trafficking offences (noted by Frances Haugen's whistleblowing evidence) are a serious omission from Schedule 7 that should be rectified. Advertising is an important route for modern indentured servitude and should clearly be in scope for that offence. We understand there are also issues with illegal organ trafficking on social media. We are aware of serious issues raised by campaigners on animal trafficking and animal cruelty which also appear to be omissions from the Schedule 7 list.
- Racism, misogyny and VAWG: If the Bill does not deal with the large-scale racism (that was short of illegality) on social media suffered by young footballers after the men's European Championships last year, then it will have failed. Harmful misogyny is not illegal but not yet tackled in the Bill; while Schedule 7 does include a list of sexual offences and aggravated offences, the Bill makes no concessions here and the wider context of Violence Against Women and Girls (VAWG) is not addressed. Working with victim representative groups we have produced a Code of Practice on Violence Against Women and Girls which could be taken up by OFCOM to work alongside the OSB regime. The code is rooted in the systems and processes approach in the Bill. The code illustrates for the first time how such a regime could work. Producing such codes gives confidence to legislators about the effect of a framework regime and enables companies to prepare for regulation. The Bill should be amended to engage the VAWG code. **As above, we will be looking further at the types of harms that might need to be included to ensure the protections required are delivered and will publish an amendment shortly.**
- Inceldom: It is unclear how the Bill will prevent the sort of radicalisation into inceldom that led to the tragic events in Plymouth in 2021. Inceldom (a newly emerging form of terrorism) is within the scope of the Prevent programme (as a mixed, unstable or unclear ideology) but we are not sure how regulated services will take account of any role they may have in a radicalisation journey. Inceldom is not mentioned specifically in the Terrorism code produced by the Home Office in 2021 and it isn't clear if inceldom fits neatly into either the code or the offence types in Schedule 5.

Issue: gaps in advertising provision

40. The new rules on fraudulent advertising are good as far as they go – but they should apply evenly to all regulated companies and be at least as strong and systemic as those for illegal content. A victim will suffer in the same way on whichever platform they get ripped off.
41. The Bill's measures will not apply to all online advertising providers. These rules do not apply to services defined by the government as 'Category 2b' – which are smaller, 'user-to-user' websites that host adverts. There is a risk that scammers will target consumers through paid-for content on these sites.
42. The legal requirement for search engines to tackle scam adverts seems less onerous than for social media platforms. All the way through the Bill search engines are subject to different, less onerous rules than user-to-user services, especially those in 'Category 1' – which are large user-to-user sites such as Twitter and Facebook. This difference can be seen here too but on top of that, the obligations on Category 2a services with regard to fraudulent ads are thinner than their obligations in relation to illegal content. Specifically for fraudulent advertising there is no equivalent of cl 24(4) which requires category 2a services to look at their design and the role that plays in harm, staff policies and practices and risk management arrangements. This raises concerns about whether the legal duty for search engines is stringent enough. Additionally, there is the

point that these rules do not apply to all search engines but only those in Category 2a.

43. Moreover, the consequences of the boundary between advertising and other content being removed is not clear. If adverts fall within the definition of user-generated content, then adverts are regulated content and the machinery behind advert delivery for user-to user services comes within scope where the content is either criminal or harmful to children or to adults. This inclusion is likely to be a step forward though there will be awkward boundaries to navigate, especially given the special regime for fraudulent ads is applicable only to some service providers and – as noted earlier – search paid for adverts do not fall in the general regime for search engines.

Issue: working with other regulators

44. Despite a significant suite of recommendations on this matter from the Joint Committee, there is no mention at all of any requirement to cooperate or coordinate with other regulatory bodies – though the ICO has been added in a few places as a statutory consultee. Curiously, there is a greater power for OFCOM to co-ordinate with overseas regulators than with British ones (Cl 97).
45. While the Government was clear in its response to the Joint Committee that OFCOM does not need a new “co-designation” power, it will need to work with other regulators – for example, the FCA in relation to OFCOM’s powers in enforcing the new duty on fraudulent advertising. This is a different relationship from co-designation. The lack of any requirement on them to do so has consequences not just for specific delivery issues, such as sharing of information between the regulators or ensuring clear lines of responsibility and cooperation in relation to evidence-gathering, horizon-scanning or enforcement; but also for upstream policy oversight.
46. For example, which department holds the ring on the policy oversight and related Ministerial advice on the implementation of the duty on fraudulent ads? DCMS, as the sponsor of OFCOM, or HMT, as the sponsor of the FCA, or Home Office, as the department with the policy responsibility for combatting fraud?
47. It would do no harm to set out in the Bill a requirement on OFCOM to define the terms of its relationships with other regulators and the power, if needed, to get them to work effectively together. **We will publish an amendment on this shortly.**

Conclusion

48. The public want action on harms²⁰ and have waited long enough to see this Bill. With the proposals we set out above, and the supporting amendments that we are drafting, we believe that version of the Bill currently before Parliament can be strengthened to better protect users online, to bolster the powers and effectiveness of the regulator and to make the system work better for regulated companies.
49. We look forward to discussing our proposals further with the Committee and would be happy to provide further information if required.

Carnegie UK
May 2022

Contact: maeve.walsh@carnegieuk.org

20 74% think the government should do more to address online harassment and violence against women and girls (<https://www.endviolenceagainstwomen.org.uk/74-think-government-should-do-more-to-ensure-social-media-platforms-address-online-abuse-of-women-and-girls/>); 70% support making it a legal requirement for platforms to assess the risks of child abuse on their services and take steps to address (<https://www.nspcc.org.uk/about-us/news-opinion/2021/poll-shows-widescale-public-support-for-stronger-laws-to-protect-children-from-online-abuse/>)